

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 in its capacity as elected Office

Date of mailing (day/month/year) 12 January 2001 (12.01.01)	
International application No. PCT/DE00/00586	Applicant's or agent's file reference F00-0432.PEM
International filing date (day/month/year) 02 March 2000 (02.03.00)	Priority date (day/month/year) 12 March 1999 (12.03.99)
Applicant NEHL, Roland	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

11 October 2000 (11.10.00)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Henrik Nyberg Telephone No.: (41-22) 338.83.38
---	---

PCT

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Internationales Aktenzeichen

Internationales Anmeldedatum

Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts (falls gewünscht)
(max. 12 Zeichen)

FOO-0432.PEM

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Anonymisierungsverfahren

Feld Nr. II ANMELDER

Name und Anschrift: (Familienname, Vorname, bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

LOK Lombardkasse AG
Grüneburgweg 102
D-60323 Frankfurt am Main

☐ Diese Person ist gleichzeitig Erfinder

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Staatsangehörigkeit (Staat):

DE

Sitz oder Wohnsitz (Staat):

DE

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

NEHL, Dr. Roland
Wiesenstraße 33
D-35789 Weilmünster

Diese Person ist:

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

DE

Sitz oder Wohnsitz (Staat):

DE

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☒ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER; ODER ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als:

☒ Anwalt

☐ gemeinsamer Vertreter

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)

MAHLER, Peter
Feddersen Laule Ewerwahn Scherzberg
Finkelnburg Clemm
Jungfernstieg 51
D-20354 Hamburg

Telefonnr.:

Telefaxnr.:
+49 40-350 05-210

Fernschreibnr.:

+49 40-350 05-128

☐ Zustellanschrift: Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

Feld Nr. V BESTIMMUNG VON STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen (bitte die entsprechenden Kästchen ankreuzen; wenigstens ein Kästchen muß angetreut werden):

Regionales Patent

- ☐ AP ARIPO-Patent: GH Ghana, GM Gambia, KE Kenia, LS Lesotho, MW Malawi, SD Sudan, SZ Swasiland, UG Uganda, ZW Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist
- ☐ EA Eurasisches Patent: AM Armenien, AZ Aserbaidshan, BY Belarus, KG Kirgisistan, KZ Kasachstan, MD Republik Moldau, RU Russische Föderation, TJ Tadschikistan, TM Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist
- ☒ EP Europäisches Patent: AT Österreich, BE Belgien, CH und LI Schweiz und Liechtenstein, CY Zypern, DE Deutschland, DK Dänemark, ES Spanien, FI Finnland, FR Frankreich, GB Vereinigtes Königreich, GR Griechenland, IE Irland, IT Italien, LU Luxemburg, MC Monaco, NL Niederlande, PT Portugal, SE Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist
- ☐ OA OAPI-Patent: BF Burkina Faso, BJ Benin, CF Zentralafrikanische Republik, CG Kongo, CI Côte d'Ivoire, CM Kamerun, GA Gabun, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauretanien, NE Niger, SN Senegal, TD Tschad, TG Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist (falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)

Nationales Patent (falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben):

- | | |
|---|---|
| <input type="checkbox"/> AL Albanien | <input type="checkbox"/> LS Lesotho |
| <input type="checkbox"/> AM Armenien | <input type="checkbox"/> LT Litauen |
| <input type="checkbox"/> AT Österreich | <input type="checkbox"/> LU Luxemburg |
| <input type="checkbox"/> AU Australien | <input type="checkbox"/> LV Lettland |
| <input type="checkbox"/> AZ Aserbaidshan | <input type="checkbox"/> MD Republik Moldau |
| <input type="checkbox"/> BA Bosnien-Herzegowina | <input type="checkbox"/> MG Madagaskar |
| <input type="checkbox"/> BB Barbados | <input type="checkbox"/> MK Die ehemalige jugoslawische Republik |
| <input type="checkbox"/> BG Bulgarien | Mazedonien |
| <input type="checkbox"/> BR Brasilien | <input type="checkbox"/> MN Mongolei |
| <input type="checkbox"/> BY Belarus | <input type="checkbox"/> MW Malawi |
| <input checked="" type="checkbox"/> CA Kanada | <input type="checkbox"/> MX Mexiko |
| <input type="checkbox"/> CH und LI Schweiz und Liechtenstein | <input type="checkbox"/> NO Norwegen |
| <input type="checkbox"/> CN China | <input type="checkbox"/> NZ Neuseeland |
| <input type="checkbox"/> CU Kuba | <input type="checkbox"/> PL Polen |
| <input type="checkbox"/> CZ Tschechische Republik | <input type="checkbox"/> PT Portugal |
| <input type="checkbox"/> DE Deutschland | <input type="checkbox"/> RO Rumänien |
| <input type="checkbox"/> DK Dänemark | <input type="checkbox"/> RU Russische Föderation |
| <input type="checkbox"/> EE Estland | <input type="checkbox"/> SD Sudan |
| <input type="checkbox"/> ES Spanien | <input type="checkbox"/> SE Schweden |
| <input type="checkbox"/> FI Finnland | <input type="checkbox"/> SG Singapur |
| <input type="checkbox"/> GB Vereinigtes Königreich | <input type="checkbox"/> SI Slowenien |
| <input type="checkbox"/> GD Grenada | <input type="checkbox"/> SK Slowakei |
| <input type="checkbox"/> GE Georgien | <input type="checkbox"/> SL Sierra Leone |
| <input type="checkbox"/> GH Ghana | <input type="checkbox"/> TJ Tadschikistan |
| <input type="checkbox"/> GM Gambia | <input type="checkbox"/> TM Turkmenistan |
| <input type="checkbox"/> HR Kroatien | <input type="checkbox"/> TR Türkei |
| <input type="checkbox"/> HU Ungarn | <input type="checkbox"/> TT Trinidad und Tobago |
| <input type="checkbox"/> ID Indonesien | <input type="checkbox"/> UA Ukraine |
| <input type="checkbox"/> IL Israel | <input type="checkbox"/> UG Uganda |
| <input type="checkbox"/> IN Indien | <input checked="" type="checkbox"/> US Vereinigte Staaten von Amerika |
| <input type="checkbox"/> IS Island | |
| <input checked="" type="checkbox"/> JP Japan | <input type="checkbox"/> UZ Usbekistan |
| <input type="checkbox"/> KE Kenia | <input type="checkbox"/> VN Vietnam |
| <input type="checkbox"/> KG Kirgisistan | <input type="checkbox"/> YU Jugoslawien |
| <input type="checkbox"/> KP Demokratische Volksrepublik Korea | <input type="checkbox"/> ZW Simbabwe |
| <input type="checkbox"/> KR Republik Korea | |
| <input type="checkbox"/> KZ Kasachstan | |
| <input type="checkbox"/> LC Saint Lucia | |
| <input type="checkbox"/> LK Sri Lanka | |
| <input type="checkbox"/> LR Liberia | |

Kästchen für die Bestimmung von Staaten (für die Zwecke eines nationalen Patents), die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind:

- ☐
- ☐
- ☐

Erklärung bzgl. vorsorglicher Bestimmungen: Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der im Zusatzfeld genannten Bestimmungen, die von dieser Erklärung ausgenommen sind. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. (Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehten.)

Blatt Nr. 3

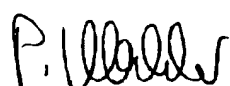
Feld Nr. VI PRIORITÄTSANSPRUCH		<input type="checkbox"/> Weitere Prioritätsansprüche sind im Zusatzfeld angegeben.		
Anmeldedatum der früheren Anmeldung (Tag/Monat/Jahr)	Aktenzeichen der früheren Anmeldung	Ist die frühere Anmeldung eine:		
		nationale Anmeldung: Staat	regionale Anmeldung: regionales Amt	internationale Anmeldung: Anmeldeamt
Zeile (1) 12.03.1999	199 11 176.6	DE		
Zeile (2)				
Zeile (3)				

☒ Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der oben in der (den) Zeile(n) 1 bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln (nur falls die frühere Anmeldung(en) bei dem Amt eingereicht worden ist(sind), das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist)

* Falls es sich bei der früheren Anmeldung um eine ARIPO-Anmeldung handelt, so muß in dem Zusatzfeld mindestens ein Staat angegeben werden, der Mitgliedsstaat der Pariser Verbandsvereinbarung zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung eingereicht wurde.

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE	
Wahl der internationalen Recherchenbehörde (ISA) (falls zwei oder mehr als zwei internationale Recherchenbehörden für die Ausführung der internationalen Recherche zuständig sind, geben Sie die von Ihnen gewählte Behörde an; der Zweibuchstaben-Code kann benutzt werden):	Antrag auf Nutzung der Ergebnisse einer früheren Recherche; Bezugnahme auf diese frühere Recherche (falls eine frühere Recherche bei der internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist): Datum (Tag/Monat/Jahr) Aktenzeichen Staat (oder regionales Amt)
ISA /	

Feld Nr. VIII KONTROLLISTE; EINREICHUNGSSPRACHE	
Diese internationale Anmeldung enthält die folgende Anzahl von Blättern:	Dieser internationalen Anmeldung liegen die nachstehend angekreuzten Unterlagen bei:
Antrag : 3	1. <input type="checkbox"/> Blatt für die Gebührenberechnung
Beschreibung (ohne Sequenzprotokollteil) : 12	2. <input type="checkbox"/> Gesonderte unterzeichnete Vollmacht
Ansprüche : 1	3. <input type="checkbox"/> Kopie der allgemeinen Vollmacht: Aktenzeichen (falls vorhanden):
Zusammenfassung : 1	4. <input type="checkbox"/> Begründung für das Fehlen einer Unterschrift
Zeichnungen : 4	5. <input type="checkbox"/> Prioritätsbeleg(e), in Feld Nr. VI durch folgende Zeilennummer gekennzeichnet:
Sequenzprotokollteil der Beschreibung : -	6. <input type="checkbox"/> Übersetzung der internationalen Anmeldung in die folgende Sprache:
Blattzahl insgesamt : 21	7. <input type="checkbox"/> Gesonderte Angaben zu hinterlegten Mikroorganismen oder anderem biologischen Material
Abbildung der Zeichnungen, die mit der Zusammenfassung veröffentlicht werden soll (Nr.): 4	8. <input type="checkbox"/> Protokoll der Nucleotid- und/oder Aminosäuresequenzen in computerlesbarer Form
	9. <input type="checkbox"/> Sonstige (einzeln auflisten):
	Sprache, in der die internationale Anmeldung eingereicht wird: DE

Feld Nr. IX UNTERSCHRIFT DES ANMELDERS ODER DES ANWALTS	
Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.	
 MAHLER, Peter Patentanwalt	

Vom Anmeldeamt auszufüllen	
1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung:	2. Zeichnungen <input type="checkbox"/> eingegangen: <input type="checkbox"/> nicht eingegangen:
3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:	
4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:	
5. Internationale Recherchenbehörde (falls zwei oder mehr zuständig sind): ISA /	6. <input type="checkbox"/> Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchegebühr aufgeschoben

Vom Internationalen Büro auszufüllen	
Datum des Eingangs des Aktenexemplars beim Internationalen Büro:	

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts 1343 PCT	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/DE 00/01294	Internationales Anmeldedatum (Tag/Monat/Jahr) 26/04/2000	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 30/04/1999
Anmelder ZF LEMFÖRDER METALLWAREN AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

☐ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☒ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

☒ wie vom Anmelder vorgeschlagen

☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

☐ keine der Abb.

Translation
09/936410

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference F00-0432.PEM	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE00/00586	International filing date (day/month/year) 02 March 2000 (02.03.00)	Priority date (day/month/year) 12 March 1999 (12.03.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/00		
Applicant LOK LOMBARDKASSE AG		

<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet.</p> <p><input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of _____ sheets.</p>
<p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input checked="" type="checkbox"/> Certain defects in the international application</p> <p>VIII <input type="checkbox"/> Certain observations on the international application</p>

Date of submission of the demand 11 October 2000 (11.10.00)	Date of completion of this report 07 March 2001 (07.03.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE00/00586

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

- ☐ the international application as originally filed.
- ☒ the description, pages 1-12, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.
- ☒ the claims, Nos. 1-7, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____,
Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig 1/4-4/4, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims	1-7	YES
	Claims		NO
Inventive step (IS)	Claims	1-7	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-7	YES
	Claims		NO

2. Citations and explanations**1. Claim 1**

The invention relates to a method for the anonymization of sensitive data within a data stream.

In the known methods for protecting databases, either access to the whole data base is denied or selective control over access to certain data is assigned to an administrator.

The problem addressed by the present invention is that of creating a method which allows access to a database, but, in so doing, excludes access to certain data within the database, without disturbing the way the excluded data are assigned with respect to the remaining data. It should be possible to entrust the database to the hands of third parties for the processing of the non-protected data without control of access to the protected data being handed over at the same time.

The sensitive data field within a data stream is first compressed and then anonymized, thus creating

space. Identification of said anonymized sensitive data stream is then carried out by means of start and stop signs, said identification being necessary for later deanonymization of the data field. In this way the sensitive data within a database are selectively anonymized. The method as per the invention can be used in particular if a database user deposits data in a database and parts of the data are supposed to be processed by a database operator. By using the method as per the invention, the non-anonymized data can be evaluated and processed by the database operator, the anonymization information can remain with the database user and the way the data are assigned to each other can be upheld.

The citations from the international search report do not disclose or suggest the concept underlying the invention.

The subject matter of Claim 1 is therefore novel and inventive (PCT Article 33(2) and (3)).

2. Claims 2 to 7

Dependent Claims 2 to 7 contain further details of the method for the anonymization of sensitive data of a data stream as per Claim 1. Since said claims are dependent on Claim 1, they also meet the requirements for novelty and inventive step as per PCT Article 33(2) and (3).

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. A document that reflects the prior art described on pages 1 and 2 was not cited in the description (PCT Rule 5.1(a)(ii)). Document US-A-5 768 391, which was cited in the international search report, would be considered to represent general prior art.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts F00-0432.PEM	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/DE 00/ 00586	Internationales Anmeldedatum (Tag/Monat/Jahr) 02/03/2000	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 12/03/1999
Anmelder LOK LOMBARDKASSE AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.
- ☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.
- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das
- ☐ in der internationalen Anmeldung in Schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der Bezeichnung der Erfindung

- ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
- ☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der Zusammenfassung

- ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
- ☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 4

- ☒ wie vom Anmelder vorgeschlagen
- ☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
- ☐ weil diese Abbildung die Erfindung besser kennzeichnet.
- ☐ keine der Abb.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 F16F13/30

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 F16F B60K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

WPI Data, PAJ, EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 312 719 A (FREUDENBERG CARL FA) 26. April 1989 (1989-04-26) Abbildungen 7,8 Spalte 8, Zeile 43 -Spalte 9, Zeile 16 ----	1
A	US 5 060 919 A (TAKANO KAZUYA ET AL) 29. Oktober 1991 (1991-10-29) das ganze Dokument ----	1
A	DE 196 17 839 A (METZELER GIMETALL AG) 13. November 1997 (1997-11-13) in der Anmeldung erwähnt -----	



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

4. September 2000

Absendedatum des internationalen Recherchenberichts

11/09/2000

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Beaumont, A

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 00/01294

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0312719	A	26-04-1989	DE 3735553 A	03-05-1989
			BR 8805433 A	27-06-1989
			DE 3744916 C	05-03-1992
			DE 3867204 A	06-02-1992
			ES 2027737 T	16-06-1992
			JP 1153832 A	16-06-1989
			JP 2539895 B	02-10-1996
US 5060919	A	29-10-1991	JP 2617715 B	04-06-1997
			JP 63266237 A	02-11-1988
DE 19617839	A	13-11-1997	NONE	

Feld III

WORTLAUT DER ZUSAMMENFASSUNG (Fortsetzung von Punkt 5 auf Blatt 1)

Die Zusammenfassung wird wie folgt geändert:

- Zeile 2: nach "Arbeitskammer" wird "(1)" eingefügt;
- Zeile 3: nach "Ausgleichskammer" wird "(2)" eingefügt;
- Zeile 4: nach "Überströmkanal" wird "(8)" eingefügt;
- Zeile 10: nach "Trägerschicht" wird "(10)" eingefügt;
- Zeile 11: nach "Deckschichten" wird "(11,12)" eingefügt.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

REC'D 09 MAR 2001

WIPO

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)



Aktenzeichen des Anmelders oder Anwalts F00-0432.PEM.ras	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE00/00586	Internationales Anmeldedatum (Tag/Monat/Jahr) 02/03/2000	Prioritätsdatum (Tag/Monat/Tag) 12/03/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/00		
Anmelder LOK LOMBARDKASSE AG et al.		

- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.
 - ☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 11/10/2000	Datum der Fertigstellung dieses Berichts 07.03.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Bertini, S Tel. Nr. +49 89 2399 8985 

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-12 ursprüngliche Fassung

Patentansprüche, Nr.:

1-7 ursprüngliche Fassung

Zeichnungen, Blätter:

1/4-4/4 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE00/00586

- ☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-7
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-7
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-7
	Nein: Ansprüche	

2. Unterlagen und Erklärungen siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

**V. BEGRÜNDETE FESTSTELLUNG NACH ARTIKEL 35 (2) HINSICHTLICH DER NEUHEIT, DER
ERFINDERISCHEN TÄTIGKEIT UND DER GEWERBLICHEN ANWENDBARKEIT; UNTERLAGEN UND
ERKLÄRUNGEN ZUR STÜTZUNG DIESER FESTSTELLUNG**

1. Anspruch 1

Die Erfindung bezieht sich auf ein Verfahren zur Anonymisierung sensibler Daten innerhalb eines Datenstroms.

Bei den bekannten Verfahren zum Schutz von Datenbanken wird entweder der Zugriff auf die gesamte Datenbank unterbunden oder die selektive Kontrolle über den Zugriff auf bestimmte Daten einem Administrator unterstellt. Grundsätzlich wäre der Zugriff somit auch auf sensible Daten möglich.

Die Aufgabe der vorliegenden Erfindung ist ein Verfahren zu schaffen, welches den Zugriff auf eine Datenbank ermöglicht, dabei aber bestimmte Daten innerhalb dieser Datenbank vom Zugriff ausschließt, ohne die Zuordnung der ausgeschlossenen Daten zu den restlichen Daten zu zerstören. Die Datenbank soll zur Bearbeitung der nicht geschützten Daten in dritte Hände gegeben werden können, ohne daß die Zugriffskontrolle auf die geschützten Daten aus der Hand gegeben wird.

Das sensible Datenfeld innerhalb eines Datenstroms wird zuerst komprimiert und dann anonymisiert; somit wird Platz geschaffen. Danach wird eine Kennzeichnung dieses anonymisierten sensiblen Datenfeldes innerhalb des Datenstroms durch Start- und Stoppzeichen durchgeführt, welche zur späteren Deanonymisierung des Datenfeldes notwendig ist. Somit werden die sensiblen Daten innerhalb einer Datenbank selektiv anonymisiert. Das erfindungsgemäße Verfahren kann insbesondere eingesetzt werden, wenn ein Datenbanknutzer Daten in einer Datenbank ablegt, und Teile der Daten durch einen Datenbankbetreiber bearbeitet werden sollen. Durch das erfindungsgemäße Verfahren, können die nicht anonymisierten Daten vom Datenbankbetreiber ausgewertet und bearbeitet werden, die Anonymisierungsinformation beim Datenbanknutzer verbleiben und dazu kann die Zuordnung der Daten zueinander erhalten bleiben.

Das Anmeldungskonzept wird durch die im Internationalen Recherchenbericht genannten Druckschriften weder offenbart noch nahegelegt.

Der Gegenstand des Anspruchs 1 ist daher neu und erfinderisch (Artikel 33 (2) und (3) PCT).

2. Ansprüche 2 bis 7

Die abhängigen Ansprüche 2 bis 7 enthalten weitere Details des Verfahrens zur Anonymisierung sensibler Daten eines Datenstroms gemäß Anspruch 1. Da sie vom Anspruch 1 abhängig sind, erfüllen auch sie die Erfordernisse gemäß PCT (Artikel 33 (2) und (3)) bezüglich Neuheit und erfinderischer Tätigkeit.

VII. BESTIMMTE MÄNGEL DER INTERNATIONALEN ANMELDUNG

1. Ein Dokument, das den auf Seiten 1 und 2 beschriebenen Stand der Technik widerspiegelt, wurde in der Beschreibung nicht angegeben (Regel 5.1 a) ii) PCT). Als allgemeiner Stand der Technik wäre das im Internationalen Recherchenbericht zitierte Dokument US-A-5 768 391 anzugeben.



<p>(51) Internationale Patentklassifikation ⁷ : H04L 9/00</p>	A2	<p>(11) Internationale Veröffentlichungsnummer: WO 00/56005</p> <p>(43) Internationales Veröffentlichungsdatum: 21. September 2000 (21.09.00)</p>
<p>(21) Internationales Aktenzeichen: PCT/DE00/00586</p> <p>(22) Internationales Anmeldedatum: 2. März 2000 (02.03.00)</p> <p>(30) Prioritätsdaten: 199 11 176.6 12. März 1999 (12.03.99) DE</p> <p>(71) Anmelder (für alle Bestimmungsstaaten ausser US): LOK LOMBARDKASSE AG [DE/DE]; Grüneburgweg 102, D-60323 Frankfurt am Main (DE).</p> <p>(72) Erfinder; und</p> <p>(75) Erfinder/Anmelder (nur für US): NEHL, Roland [DE/DE]; Wiesenstrasse 33, D-35789 Weilmünster (DE).</p> <p>(74) Anwalt: MAHLER, Peter; Feddersen Laule Ewerwahn Scherzberg Finkelnburg Clemm, Jungfernstieg 51, D-20354 Hamburg (DE).</p>		<p>(81) Bestimmungsstaaten: CA, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>Veröffentlicht <i>Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.</i></p>
<p>(54) Title: ANONYMIZATION METHOD</p> <p>(54) Bezeichnung: ANONYMISIERUNGSVERFAHREN</p> <div style="text-align: center; margin-top: 20px;"> <pre> graph TD subgraph TopRow [] direction LR QS[QUANTITY START SIGN] --- EDF[ENCRYPTED DATA FIELD] --- SS[STOP SIGN] end QS --- MS[Menge Startzeichen] EDF --- VDF[Verschlüsseltes Datenfeld] SS --- SZ[Stopppzeichen] MS --- A[Schlüssel-Nummer A] VDF --- B[Codierter Initialisierungsvektor B] VDF --- C[Geheimtext C] C --- D[Komprimiertes Datenfeld D] D --- VM[Verschlüsselungsverfahren] VM --- EM[ENCRYPTION METHOD] </pre> <p style="margin-top: 10px;"> A...KEY NUMBER B...CODED INITIALIZATION VECTOR C...SECRET TEXT D...COMPRESSED DATA FIELD </p> </div>		
<p>(57) Abstract</p> <p>The invention relates to a method for rendering anonymous sensitive data within a data stream. The invention provides a method which comprises the following steps: Compressing the sensitive data field; rendering anonymous the sensitive data field, and distinguishing the anonymized sensitive data field within the data stream by means of start and stop signs.</p>		

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Anonymisierung sensibler Daten innerhalb eines Datenstroms. Erfindungsgemäß wird ein Verfahren vorgeschlagen, das die Schritte Komprimierung des sensiblen Datenfeldes, Anonymisierung des sensiblen Datenfeldes und Kennzeichnung des anonymisierten sensiblen Datenfeldes innerhalb des Datenstroms durch Start- und Stopzeichen umfaßt.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshjan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Anonymisierungsverfahren

Die Erfindung betrifft ein Verfahren zur Anonymisierung sensibler Daten innerhalb eines Datenstroms.

- 5 In Datenbanken werden Informationen zur langfristigen Aufbewahrung gespeichert. Der Wert solcher Informationssammlungen wird als wesentliches Gut von Organisationen angesehen. Aufgrund der Sensitivität wird im allgemeinen der Zugriff auf Datenbanken beschränkt, d.h. daß der Zugriff nur für autorisierte Anwender gemäß deren Rechteprofil möglich ist. In einem Rechteprofil kann festgelegt werden, wer auf
- 10 welche Daten mit welchen Modi (z.B. lesend, schreibend) zugreifen kann. Ein gängiges Beispiel ist, daß nicht jeder Mitarbeiter eines Unternehmens Personaldaten einsehen kann. Auch gemäß dem „Need to know“-Prinzip können Mitarbeiter ausschließlich die Informationen einsehen, die sie zur Ausübung ihrer dienstlichen Tätigkeiten benötigen. Alle weiteren Informationen sind gesperrt. Für die Vergabe der
- 15 Zugriffsrechte ist ein Administrator zuständig, von dessen Zuverlässigkeit der Datenschutz im wesentlichen abhängt.

- Zur Datensicherung werden häufig Anonymisierungsverfahren eingesetzt, die diejenigen Daten, auf die kein Zugriff erfolgen soll, anonymisieren. Solche Verfahren werden insbesondere verwendet, wenn Daten einer Datenbank in Form eines
- 20 Datenstroms übermittelt werden sollen, wobei sichergestellt werden muß, daß auf dem Übermittlungsweg kein unberechtigter Zugriff auf die Daten erfolgt. Ein Anwendungsbeispiel hierfür ist die Versendung eines Datenstroms per E-Mail. Dabei haben Sender und Empfänger volle Zugriffsrechte auf alle in der Datenbank enthaltenen Daten. Die Daten werden vor Absendung verschlüsselt, so daß Angreifer
- 25 innerhalb des Internets keinen Zugriff auf die Daten nehmen können. Der Empfänger entschlüsselt die Daten und kann vollständigen Zugriff darauf nehmen.

- Bei den bekannten Verfahren zum Schutz von Datenbanken wird die Autorisierung und Rechteprüfung typischerweise am Datenbank-Front End realisiert. Dies trifft z.B. für DB2™ von IBM zu. Wird ein höheres Niveau bzgl. des Zugriffsschutzes gefordert, so
- 30 gibt es kommerzielle Produkte, wie z.B. RACF™ (Ressource Access Control Facility) von IBM. Die Zugriffskontrolle wird jedoch auch hier von einem Administrator kontrolliert.

Eine klassische Situation, in der die herkömmlichen Verfahren unzureichend sind, ist eine Outsourcer/Insourcer-Beziehung. Ein Outsourcer läßt bestimmte Dienste durch

- einen Insourcer erbringen und übergibt dem Insourcer alle dafür notwendigen Daten, die beim Insourcer in einer Datenbank gespeichert werden. Wenn der Outsourcer aus Datenschutzgründen oder aus Gründen des Kundenschatzes die Weitergabe von kundenidentifizierenden Daten eigenständig kontrollieren will, wird mit den bekannten
- 5 Anonymisierungsverfahren entweder der Zugriff auf die gesamte Datenbank unterbunden oder die selektive Kontrolle über den Zugriff auf bestimmte Daten einem Administrator unterstellt, der im dem Hause des Insourcers angesiedelt ist. Grundsätzlich wäre der Zugriff somit auch auf sensible Daten möglich.

- Es ist Aufgabe der vorliegenden Erfindung, ein Verfahren zur Verfügung zu stellen,
- 10 das den Zugriff auf eine Datenbank ermöglicht, dabei aber bestimmte Daten innerhalb dieser Datenbank vom Zugriff ausschließt, ohne die Zuordnung der ausgeschlossenen Daten zu den restlichen Daten zu zerstören. Die Datenbank soll zur Bearbeitung der nicht geschützten Daten in dritte Hände gegeben werden können, ohne daß die Zugriffskontrolle auf die geschützten Daten aus der Hand gegeben wird.

- 15 Erfindungsgemäß wird ein Verfahren zur Anonymisierung sensibler Daten innerhalb eines Datenstroms mit folgenden Schritten vorgeschlagen:

- a) Komprimierung des sensiblen Datenfeldes
 - b) Anonymisierung des sensiblen Datenfelds;
 - c) Kennzeichnung des anonymisierten sensiblen Datenfelds innerhalb des
- 20 Datenstroms durch Start- und Stoppzeichen.

Erfindungsgemäß werden die sensiblen Daten innerhalb einer Datenbank selektiv anonymisiert. Die anonymisierten Datenfelder werden mit einem Start- und einem Stoppzeichen versehen, um sie für die spätere Deanonymisierung kenntlich zu machen.

- 25 Das erfindungsgemäße Verfahren kann insbesondere eingesetzt werden, wenn ein Datenbanknutzer Daten in einer Datenbank ablegt, und Teile der Daten durch einen Datenbankbetreiber bearbeitet werden sollen. Während der Datenbanknutzer autorisiert ist, sämtliche Daten zu lesen, sollen sensible Daten, wie z. B. kundenidentifizierende Informationen, für den Datenbankbetreiber anonymisiert und
- 30 nicht deanonymisierbar sein. Die Anonymisierungsinformation verbleibt beim Datenbanknutzer. Die nicht anonymisierten Daten können vom Datenbankbetreiber ausgewertet und bearbeitet werden. Die Zuordnung der Daten zueinander bleibt erhalten.

Die sensiblen Daten können beispielsweise kundenidentifizierende Informationen sein, wobei die dem Kunden zugeordneten Daten zwecks statistischer Auswertung lesbar sein sollen. Die Datenbank kann mit dem erfindungsgemäßen Anonymisierungsverfahren partiell anonymisiert und an Dritte zur statistischen Auswertung und
5 Bearbeitung weitergegeben werden. Die kundenidentifizierenden Daten sind für den Dritten nicht lesbar. Die Kontrolle darüber, welche Zugriffsrechte für welche Personen bestehen, verbleibt beim Datenbanknutzer. Die Zuordnung zwischen den bearbeiteten Daten und den jeweiligen anonymisierten Daten, wie Kundennamen, bleibt erhalten. Nach Rückgabe der ausgewerteten oder bearbeiteten Datenbank an den
10 Datenbanknutzer kann dieser die Deanonymisierung vornehmen und die vollständige, bearbeitete Datenbank nutzen.

Das erfindungsgemäße Verfahren läßt sich insbesondere auch dann vorteilhaft anwenden, wenn die sensiblen Datenfelder eine vorgegebene Feldlänge aufweisen. Es versteht sich aber von selbst, daß das Verfahren ohne Einschränkung auch bei
15 unbegrenzten Feldlängen entsprechend anwendbar ist. Auch wenn sich die nachfolgenden Ausführungen vermehrt auf sensible Datenfelder vorgegebener Feldlänge beziehen, ist dies nicht einschränkend zu verstehen.

Vorteilhaft kann vor der Anonymisierung des sensiblen Datenfeldes eine Komprimierung der Daten vorgenommen werden. Im Falle der vollständigen Füllung
20 des Datenfeldes wird auf diesem Wege Platz für die Hinzufügung von Start- und Stoppzeichen zur Kennzeichnung des anonymisierten Datenfeldes geschaffen. Die Kennzeichnung ist notwendig zur späteren Deanonymisierung des Datenfeldes.

Ist das Datenfeld ohnehin nicht vollständig gefüllt, oder sind die Daten durch die Komprimierung soweit komprimiert, daß noch Platz im Datenfeld verbleibt, kann das
25 Datenfeld vor der Anonymisierung durch Füllzeichen aufgefüllt werden.

Es stehen insbesondere zwei Möglichkeiten zur Anonymisierung des Datenfeldes zur Verfügung, nämlich die Pseudonymisierung und die Verschlüsselung.

Ist das Datenfeld vollständig gefüllt, wird vorzugsweise eine Pseudonymisierung vorgenommen. Dabei muß die Länge des verwendeten Pseudonyms so gewählt
30 werden, daß im Datenfeld nach der Pseudonymisierung Platz für Start- und Stoppzeichen verbleibt.

Verbleibt innerhalb des Datenfeldes noch Platz, so wird das Datenfeld vorzugsweise durch Füllzeichen, insbesondere mit zufälligen Werten, zumindest teilweise aufgefüllt und anschließend verschlüsselt.

Die Auffüllung des Feldes mit zufälligen Werten sichert die Auflösung von Isonomien. Beispielsweise ist es erforderlich, daß häufig auftretende Namen, wie im deutschen Sprachraum Müller, Meier usw. verschieden verschlüsselt werden, damit über eine Analyse der Häufigkeit der Daten keine Rückschlüsse auf die Daten gezogen werden
5 kann. Dies wird mit der Auffüllung des Datenfeldes durch zufällige Werte und anschließende Verschlüsselung erreicht.

In einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens werden im verschlüsselten Datenfeld auch Informationen über den zur Verschlüsselung verwendeten Schlüssel abgelegt. Diese Schlüsselinformationen dienen dem
10 Datenbanknutzer dazu, die verschlüsselten Daten entschlüsseln zu können. Auf diesem Wege können verschiedene Schlüssel zur Verschlüsselung der Daten verwendet werden, wobei jeweils innerhalb des Feldes die entsprechenden Schlüsselinformationen zur Identifizierung des Schlüssels abgelegt werden. Es versteht sich von selbst, daß der Füllgrad des Feldes so beschaffen oder durch
15 Datenkompression erzeugt werden muß, daß Platz zum Ablegen einer Schlüsselinformation verbleibt.

Das Erkennen, welche Daten zu ver- bzw. entschlüsseln sind, kann durch eindeutige Kennzeichnung durch sogenannte Start- und Stoppzeichen, wie z.B. „{“ und „}“ realisiert werden. Diese Start- und Stoppzeichen dürfen im betroffenen System außer
20 zur Kennzeichnung verschlüsselter Daten nicht verwendet werden. Dieser Ansatz hat den Vorteil, daß er unabhängig von den Anwendungen, die auf den Daten operieren, ist.

Gibt es im betrachteten System kein einziges eindeutiges Startzeichen, kann eine Menge von Startzeichen verwendet werden. Gleiches gilt für das Stoppzeichen. Im
25 einfachsten Fall könnte die Menge der Startzeichen aus einem Zeichen bestehen, welches mit dem Stoppzeichen identisch ist. Dies hat allerdings wiederum den Nachteil, daß eine Synchronisierung in einem Fehlerfall alleine aufgrund der Kenntnis von Start- und Stoppzeichen nicht mehr möglich ist.

Das erfindungsgemäße Verfahren wird im folgenden anhand von verschiedenen
30 Beispielen mit Bezug auf die beigefügten Abbildungen näher erläutert:

Fig. 1 zeigt die Kennzeichnung von sensiblen, zu anonymisierenden Daten;

Fig. 2 zeigt das Ablaufschema einer Ver- bzw. Entschlüsselung;

Fig. 3 zeigt den Ablauf eines Verschlüsselungsprozesses;

Fig. 4 zeigt die Struktur eines verschlüsselten Datenfeldes;

Fig. 5 zeigt den Ablauf eines Entschlüsselungsprozesses.

Das Anonymisierungsverfahren soll folgende Anforderungen erfüllen:

1. Häufig vorkommende Daten (z.B. die häufig auftretenden Namen Müller, Meier
5 usw. im deutschen Sprachraum) sollen verschieden verschlüsselt werden. Dadurch soll verhindert werden, daß über die Analyse der Häufigkeit von Daten Schlüsse auf die Daten selbst gezogen werden können. Die Isomien der Daten sollen aufgelöst werden.
2. Die Länge eines zu verschlüsselnden Datenfelds ist durch eine fixe, maximale
10 Länge beschränkt, die im wesentlichen durch das Datenbank-Design vorgegeben ist. Feldtypen, z.B. numerisch oder alphanumerisch dürfen nicht verändert werden. Diese Anforderung ermöglicht eine nachträgliche Integration des Verfahrens, ohne daß ein Betreiber eines Datenbanksystems seine Anwendungen zur Verarbeitung der Daten verändern muß.
- 15 3. Jedes verschlüsselte Datenfeld enthält alle Informationen außer Schlüssel und systemweite Parameter zur Entschlüsselung. Ein autarkes Verarbeiten jedes Datenfeldes ist deshalb möglich.

Die vorgenannten drei Eigenschaften sollen von dem gewählten Anonymisierungsverfahren gleichzeitig erfüllt werden.

- 20 Zur Durchführung des Verfahrens wird das zu anonymisierende Datenfeld zunächst auf seinen Füllgrad hin überprüft. Es muß sichergestellt werden, daß nach der Verschlüsselung noch genügend Platz innerhalb der vorgegebenen festen Datenfeldlänge verbleibt, um ein Start- sowie ein Stoppzeichen und eine Information für den verwendeten Schlüssel abzulegen.
- 25 Ist der Füllgrad des Datenfeldes zu groß um eine Verschlüsselung mit den vorgenannten Kriterien durchführen zu können, wird das Datenfeld zunächst komprimiert. Führt auch die Komprimierung des Datenfeldes nicht zu einer hinreichend kleinen Feldgröße, erfolgt die Pseudonymisierung. Das Pseudonym muß so gewählt werden, daß die oben unter 2.) vorgegebene Bedingung hinsichtlich des
30 Füllungsgrades des Datenfeldes erfüllt wird.

Ist der Füllgrad des Datenfeldes hinreichend gering, um eine Verschlüsselung des Datenfeldes zu ermöglichen, wird die Verschlüsselung vorgenommen. Dafür wird das

Datenfeld zunächst bis zum maximal möglichen Füllgrad mit zufälligen Werten aufgefüllt.

- Bei geringem Informationsgehalt des Datenfelds kann vor der Auffüllung eine Datenkomprimierung vorgenommen werden, um Isonomien besser auflösen zu können.

Anschließend wird die Verschlüsselung vorgenommen. Der verwendete Verschlüsselungsalgorithmus kann beliebig gewählt werden. Gängige Algorithmen sind z.B. IDEA (International Data Encryption Algorithm) oder DES (Data Encryption Standard).

- 10 Das verschlüsselte Datenfeld wird dann mit einem Start- und einem Stoppzeichen gekennzeichnet. Außerdem wird im Datenfeld an einer vorher definierten Position eine Information über den zur Verschlüsselung verwendeten Schlüssel abgelegt.

Das nachfolgende Beispiel soll das Verfahren veranschaulichen:

- 15 Die Datenfeldlänge beträgt 40 Zeichen. Inhalt des unverschlüsselten Datenfeldes ist der Name „Meier“. Als Startzeichen dient „{“, als Stoppzeichen „}“. Das Datenfeld wird auf die volle Feldlänge aufgefüllt und mit Start- und Stoppzeichen versehen, also:

{Meier.....}.

- An das Verfahren werden die 40 Zeichen zwischen den Start- und Stoppzeichen übergeben. Die Verschlüsselung ergibt dann ein 40 Zeichen langes Datenfeld einschließlich Start- und Stoppzeichen, also z.B.:

{ch74nHhdjqa.....yjas8}.

- 25 In den verschlüsselten Datenfeldern sind k Bits zur Kennzeichnung des verwendeten Schlüssels aus einem Schlüsselsatz vorgesehen. Somit ist es möglich, 2^k verschiedene Schlüssel darzustellen. Durch die Aufnahme von Zusatzinformationen in die verschlüsselten Datenfelder, wie z.B. Menge von Start- und von Stoppzeichen, Schlüsselbits und Informationen über den verwendeten Initialisierungssektor für den Verschlüsselungsalgorithmus ist eine Komprimierung der zu verschlüsselnden Datenfelder notwendig.

- 30 In der beigefügten Fig. 2 ist die Ver- bzw. Entschlüsselung von Datenfeldern dargestellt. Die einzelnen Schritte werden nachfolgend näher erläutert.

Die Beschreibung des Verfahrens geht von den folgenden Voraussetzungen aus:

- Jedes Zeichen wird durch ein Byte dargestellt (z.B. ASCII- oder EBCDIC-Code). Vor der Ver- bzw. Entschlüsselung werden alle Zeichen eines Feldes in einen internen Zeichensatz (ASCII) umgewandelt und danach wieder entsprechend konvertiert.
- 5 - Die unterschiedlichen Parameter sind wie folgt festgelegt:
1. einen Zeichensatz (z.B. 91 bestimmte Zeichen des EBCDIC-Codes);
 2. eine Menge der Startzeichen und Stoppzeichen für verschlüsselte Datenfelder, die nicht im Zeichensatz enthalten sind;
 3. ein Ersatzzeichen für nicht zum Zeichensatz gehörende Zeichen (ist
10 Bestandteil des Zeichensatzes);
 4. ggf. notwendige Füllzeichen (ist Bestandteil des Zeichensatzes);
 5. Verfahrensparameter für die Kompression;
 6. Angaben darüber, wie bei nicht erfolgreicher Komprimierung das ursprüngliche Datenfeld nachverarbeitet werden soll;
 - 15 7. Angaben zur Darstellung von Bitfolgen als Folgen zulässiger Zeichen;
 8. Angaben darüber, welcher der Schlüssel aus dem Schlüsselsatz verwendet werden soll.

In Abhängigkeit von der Mächtigkeit des Zeichensatzes lassen sich einzelne Bitsegmente jeweils zu Zeichenfolgen einer bestimmten Länge umformen (zum
20 Beispiel können bei einem Zeichensatz von 91 Zeichen je 13 Bit in je 2 Zeichen effektiv umgeformt werden). Optimal wäre eine „gemeinsame“ Umformung der gesamten Bitfolge durch Betrachtung der Folge als Binärzahl und Darstellung dieser Zahl zur Basis b = Mächtigkeit des Zeichensatzes.

Im folgenden wird ein Verfahren zur effektiven Codierung einer möglichst großen
25 Bitfolge in ein Datenfeld einer vorgegebenen Länge beschrieben, das für eine Implementierung auf Systemen mit 32-Bit-Prozessoren vorgesehen ist. Zunächst wird für einen gegebenen Zeichensatz vom Umfang b vor der Grundinitialisierung einmalig folgendes berechnet („ln“ bezeichnet hierbei den natürlichen Logarithmus):

- Bestimmung des Minimalwertes von x/y für ganzzahliges y von 1 bis 32 und
30 ganzzahliges $x \geq y * \ln(2)/\ln(b)$.
Beispiel: Bei $b = 91$ erhält man ein Minimum bei $x = 2$ und $y = 13$.

- Für alle Werte x' von 1 bis $x-1$ wird das jeweilige ganzzahlige Maximum $y'(x')$ mit $y'(x') * \ln(2)/\ln(b) \leq x'$ berechnet. Außerdem wird $y'(0) := 0$ gesetzt.
Beispiel: Bei $b = 91$ und $x = 2$ erhält man $y'(1) = 6$.

Es läßt sich nun folgendermaßen eine Bitfolge in ein Datenfeld der Länge d umformen:

- 5 1. Umformung von je y Bit in je x Zeichen.
Beispiel: Bei $b = 91$ werden je 13 Bit durch je 2 Zeichen dargestellt.
 2. Falls die gegebene Datenfeldlänge d nicht durch x teilbar ist, dann werden $y'(x')$ Bit in die restlichen x' Zeichen umgeformt. Im Beispiel werden noch 6 Bit durch ein Zeichen dargestellt.
- 10 Sei s die Anzahl der verwendeten Startzeichen in den verschlüsselten Datenfeldern und

$$L(d,b,s) = L = ((d - s - 1) \text{ DIV } x) * y + y'((d - s - 1) \text{ MOD } x)$$

- die Anzahl der Bits, die sich durch Anwendung des obigen Verfahrens in ein Datenfeld der Länge $(d - s - 1)$ umformen lassen. Der Wert $(d - s - 1)$ resultiert daraus, daß im
- 15 verschlüsselten Datenfeld die Menge der Startzeichen der Länge s und das Stoppzeichen enthalten sein müssen.

Bei $d = 30$, $b = 91$ und $s = 1$ erhält man zum Beispiel $L = 14 * 13 + 0 = 182$, bei $d = 15$, $b = 91$ und $s = 3$ ergibt sich $L = 5 * 13 + y'(1) = 65 + 6 = 71$.

- $m = (L - k - \text{Länge komprimierte Bitfolge})$ sei, die nach der Kompression noch zur
- 20 Verfügung stehenden Bits, k Bits sind für die Nummer des verwendeten Schlüssels vorgesehen. Für die Kompression können die verschiedensten Methoden eingesetzt werden. In Abhängigkeit von dieser Zahl m wird festgelegt, wie der Initialisierungsvektor für die Verschlüsselung bereitgestellt und codiert wird.

- Die geeignete Wahl des Initialisierungsvektors sorgt dafür, daß Isomorphismen aufgelöst werden. Es gibt hierfür prinzipiell die folgenden Möglichkeiten, die eingesetzt werden können:
- 25

- Verwendung von Zufallszahlen
- Verwendung von Zählern.

- Zeitlich gestaffelt können verschiedene Schlüssel des aus k Schlüsseln bestehenden
- 30 Schlüsselsatzes eingesetzt werden. Bei der Verschlüsselung ist festzulegen, welcher

dieser Schlüssel verwendet werden soll. Die Schlüsselnummer wird durch k Bits kodiert.

- Wenn die aus k Bits für die Nummer des Schlüssels, den Bits für die Codierung des Initialisierungsvektors und den Bits des komprimierten Datenfeldes bestehende
- 5 Bitfolge kürzer als erforderlich sein sollte, d.h. kleiner als L ist, so wird sie am Ende mit Bits „0“ aufgefüllt, bis die maximal zulässige Bitlänge L erreicht ist.

Verschlüsselt wird der komprimierte Datenfeldinhalt.

- Die Verschlüsselung kann mit einem Blockverschlüsselungsalgorithmus erfolgen und dem gespeicherten geheimen Schlüssel im CBC-Modus, wobei der letzte Block der
- 10 Länge j (falls diese kürzer als 64 Bit ist) im CFB-Modus verschlüsselt wird (siehe z.B. ISO/IEC 10116, Informations Technologie - Modes of Operation for n -bit Block Cipher Algorithm, 1991).

- Bei der Betrachtung wird davon ausgegangen, daß die typische Blocklänge von 64 verwendet wird. Eine Verallgemeinerung auf andere Blocklängen ist offensichtlich.
- 15 Eine andere Variante, die sog. Stromverschlüsselungsalgorithmen, könnten direkt zur zeichenweisen Verschlüsselung eingesetzt werden.

Zur Bildung des verschlüsselten Datenfeldes wird schließlich die erhaltene Zeichenfolge zwischen der Menge Startzeichen und dem Stoppzeichen eingefügt.

- Sobald im Datenstrom die Startzeichenfolge erkannt wird, werden die nachfolgenden
- 20 Zeichen in einen internen Speicher gegeben, bis das Stoppzeichen erscheint.

- Falls sich unter den nachfolgenden Zeichen die Startzeichenfolge befindet, wird der Prozeß der Einspeicherung abgebrochen und bei der neuen Startzeichenfolge begonnen. Falls nach einer vorgegebenen Maximallänge noch kein Stoppzeichen festgestellt wurde, wird der Prozeß ebenfalls abgebrochen und es wird erneut nach der
- 25 nächsten Startzeichenfolge gesucht. Falls zwischen der Menge Startzeichen und dem Stoppzeichen weniger als eine vordefinierte untere Schranke Zeichen sind, wird die Einspeicherung ebenfalls abgebrochen.

- Nicht jedes Datenfeld kann so stark komprimiert werden, daß die angestrebte Anzahl Bits für den Initialisierungsvektor zur Verfügung steht. Je kürzer die Datensatzlänge ist,
- 30 desto schlechter ist die Komprimierung, mit der Konsequenz, daß weniger Bits für den Initialisierungsvektor zur Verfügung stehen und somit weniger Möglichkeiten verschiedene Chiffre für ein Datenfeld zu erzeugen.

In einem solchen Fall gibt es prinzipiell die folgenden drei Möglichkeiten fortzufahren:

1. Kürzung des Datenfeldes bis eine ausreichende Komprimierung erreicht werden kann. Dies ist aber zwangsläufig mit Informationsverlust verbunden.
2. Das betroffene Datenfeldes wird nicht verschlüsselt, es wird somit in Klartext bleiben. Dies kann möglicherweise akzeptabel sein, falls dies im Verhältnis zu der gesamten Menge zu verschlüsselten Datenfelder sehr selten vorkommt.
3. Verwendung des Pseudonymisierungsansatzes, dieser wird im folgenden beschrieben.

Bei vorgegebener fester Feldlänge, kann der Fall eintreten, daß keine ausreichende Komprimierung der Datensätze erreicht werden kann. Ist eine Kürzung oder das Weiterleiten in Klartext nicht akzeptabel, so kann die vollständige "Verschleierung" aller ausgewählten Datensätze, durch den Pseudonymisierungsansatz realisiert werden.

Analog zu einem Alias, erfolgt eine Verknüpfung von Datenfeldern und Pseudonymen und vice versa. Die Informationen werden in einer Tabelle gehalten.

15	Leutheusser-Schnarrenberger	<->	X1BXE.....H
	Garmisch-Partenkirchen	<->	X2BXD9.....Z

Falls die Pseudonymisierung an mehreren räumlich getrennten Orten notwendig ist, müssen die an allen Standorten vergebenen Pseudonyme an allen anderen Standorten vorgehalten werden (Replikation). Dies bedeutet zusätzliche Kommunikationskosten. Es sind zusätzliche Maßnahmen zur Sicherung der Übertragung notwendig.

Die Speicherung von verschlüsselten Datenfeldern kann über längere Zeiträume, z.B. 5 – 15 Jahre, erfolgen. Die zeitlich gestaffelte Verwendung von mehr als einem Schlüssel ist aus den folgenden Gründen ratsam:

- Wird der Schlüssel bekannt, ist die gesamte Menge der verschlüsselten Datenfelder als offen gelegt zu betrachten.
 - Die einem Krypto-Analysten zur Verfügung stehende Menge von verschlüsselten Datenfeldern, ist wesentlich geringer, wenn mehrere Schlüssel verwendet werden.
- Deshalb sieht das Verfahren pro Menge von Datenbanknutzern, die kooperieren, k Schlüssel vor.

In einem Trust Center (vertrauenswürdige dritte Instanz), welches das notwendige technische und organisatorische Umfeld stellt, können die Schlüssel generiert werden.

Verschiedene Mengen von Datenbanknutzern, die nicht miteinander kooperieren, sollten verschiedene Mengen von Schlüsseln haben, die keinerlei Abhängigkeit von einander haben. So ist ausgeschlossen, daß eine Menge von Datenbanknutzern auf Datenbankinformationen der anderen Menge von Datenbanknutzern zugreifen kann.

Das Key Management besteht aus folgenden Funktionen:

1. Schlüsselerzeugung

Erzeugung eines Schlüsselpakts aus k Schlüsseln. Hierfür eignet sich besonders ein Hardware Zufallszahlengenerator. Im Nachgang der Schlüsselerzeugung können die generierten Schlüssel auf ein Schlüsselaufbewahrungsmedium, z.B. eine Chip- oder PCMCIA-Karte, gespeichert werden. Diese Medien können so konfiguriert werden, daß sie die kryptographischen Berechnungen selbst ausführen oder Schlüssel erst nach vorheriger Authentisierung herausgeben.

2. Schlüsselverteilung

Vom Ort der Schlüsselgenerierung können die Schlüssel auf einem Schlüsselaufbewahrungsmedium zum Einsatzort (Endgerät) oder zur sicheren Aufbewahrung (Back-up) transportiert werden.

3. Schlüssel in Endgeräte einbringen

Ein Endgerät zeichnet sich dadurch aus, daß es die notwendigen Ver- bzw. Entschlüsselungsprozesse ausführen kann. Ein solches Gerät kann eine speziell entwickelte Hardware oder ein PC sein. Die Schlüssel können aus dem Schlüsselaufbewahrungsmedium nach vorheriger Authentisierung in ein Endgerät geladen werden oder das Endgerät kann Aufträge zur Ver- und Entschlüsselung entgegennehmen. Der letzte Fall setzt eine entsprechende Ressource des Schlüsselaufbewahrungsmediums voraus, hat aber den Vorteil, daß die Schlüssel nie das Schlüsselaufbewahrungsmedium verlassen.

4. Schlüssel vernichten:

Falls ein kooperierende Menge von Datenbanknutzern ein Schlüsselpaket aus k Schlüsseln nicht mehr benötigt, ist es möglich, die Schlüssel durch geeignete Maßnahmen zu vernichten, z.B. durch Vernichtung des Schlüsselauf-

bewahrungsmediums und Löschen des Schlüsselpakets aus den entsprechenden Endgeräten, falls vorhanden.

Patentansprüche

1. Verfahren zur Anonymisierung sensibler Daten innerhalb eines Datenstroms mit den folgenden Schritten:
 - a) Komprimierung des sensiblen Datenfeldes
 - b) Anonymisierung des sensiblen Datenfeldes.
 - c) Kennzeichnung des anonymisierten sensiblen Datenfeldes innerhalb des Datenstroms durch Start- und Stoppzeichen.
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß das sensible Datenfeld vor der Anonymisierung durch Füllzeichen aufgefüllt wird.
3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß die zu anonymisierenden Daten pseudonymisiert werden.
4. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß die zu anonymisierenden Daten verschlüsselt werden.
5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet**, daß sensible Datenfelder vor der Verschlüsselung zumindest teilweise mit zufälligen Werten aufgefüllt werden.
6. Verfahren nach Anspruch 4 oder 5, **dadurch gekennzeichnet**, daß im verschlüsselten Datenfeld Informationen über den zur Verschlüsselung verwendeten Schlüssel abgelegt werden.
7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, daß das sensible Datenfeld eine feste Feldlänge aufweist.

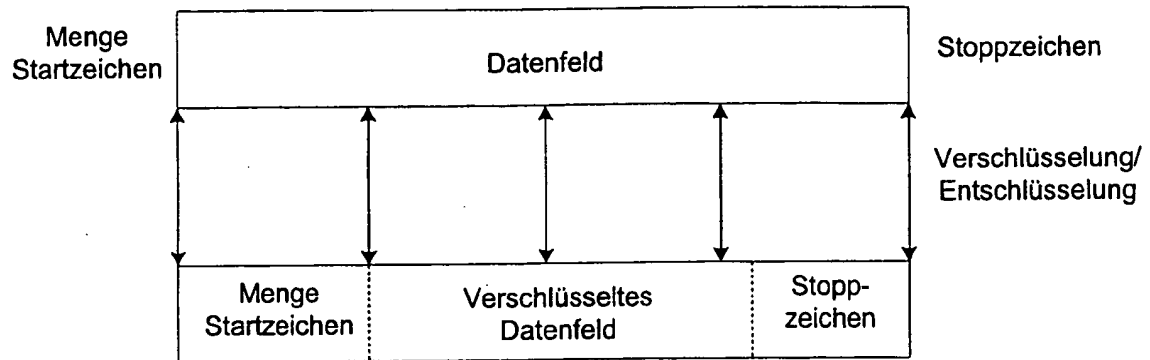


Fig. 1

5

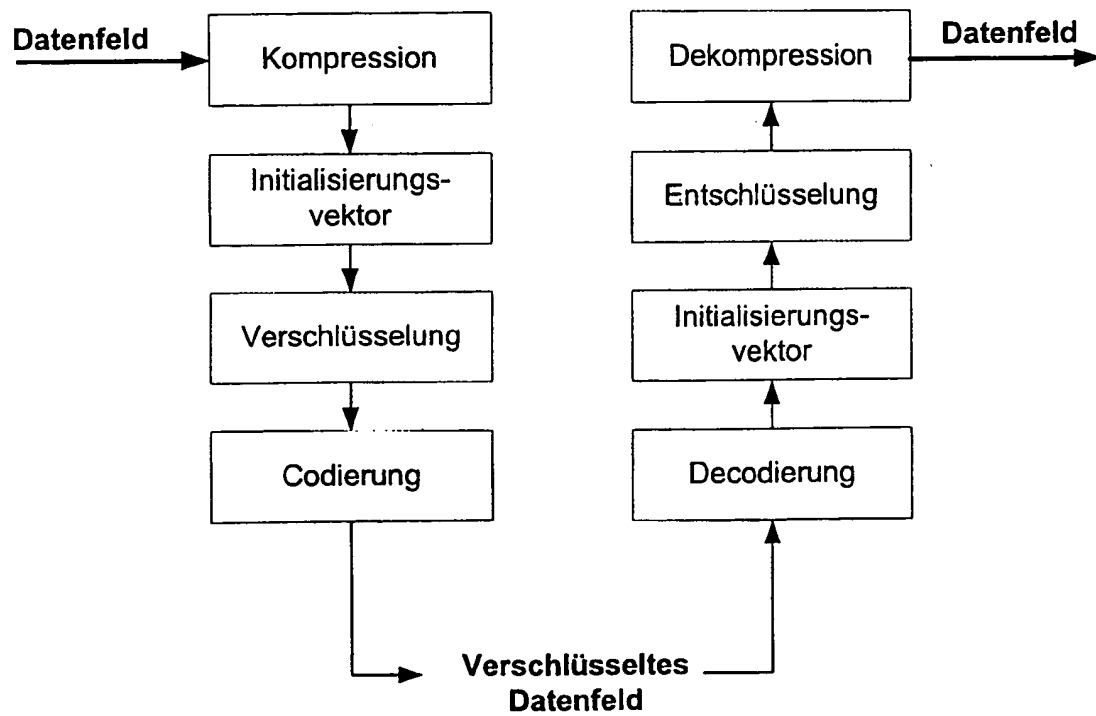


Fig. 2

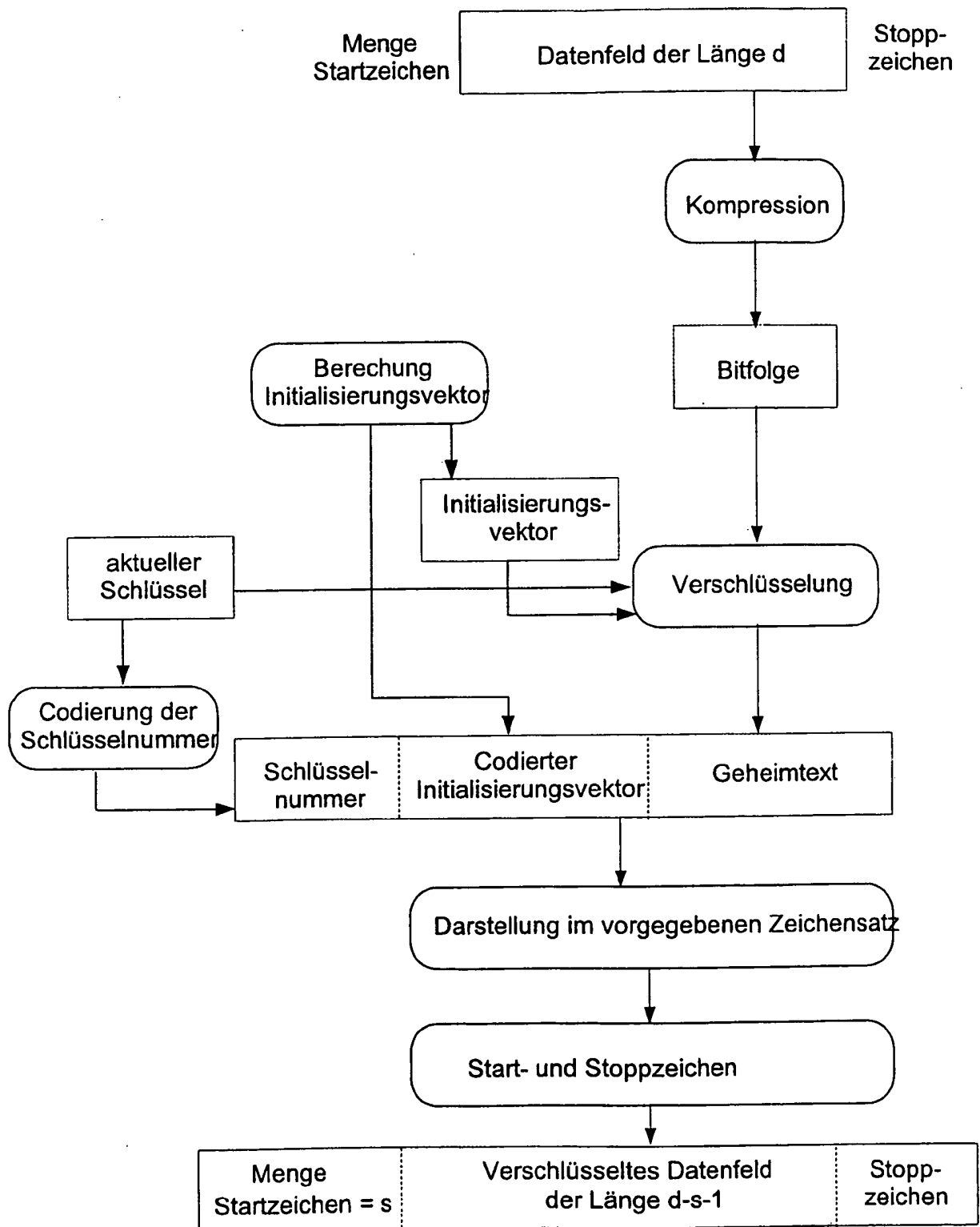


Fig. 3

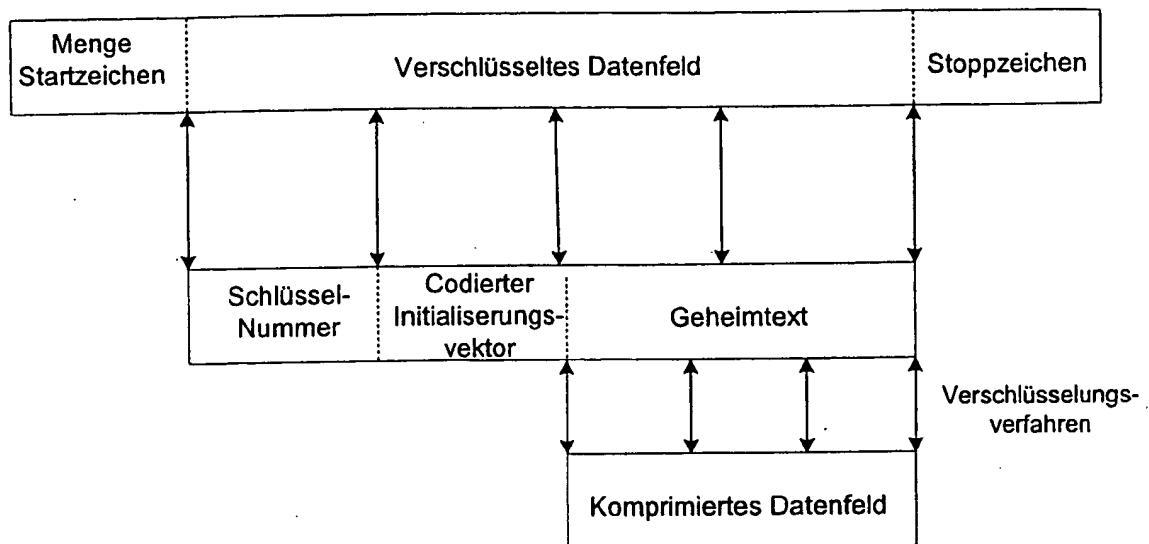


Fig. 4

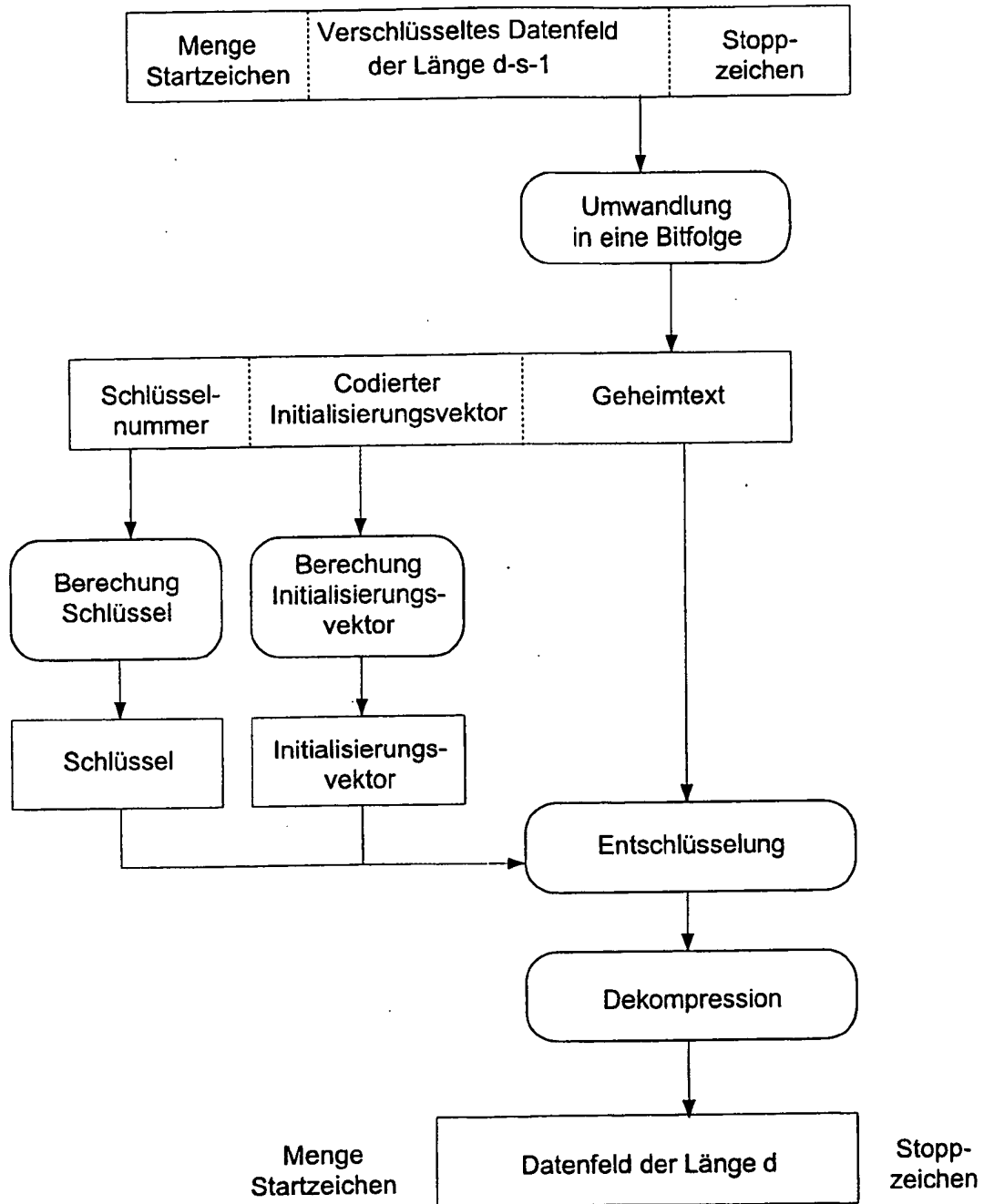


Fig. 5